IJCSMA

M.Venkatesh *et al*, International Journal of Computer Science and Mobile Applications,
Vol.2 Issue. 1, January- 2014, pg. 127-134 **ISSN: 2321-8363**

Security Analysis of Visual Secret Sharing Scheme

Mr.M.Venkatesh[1], Mr.S.Rajesh[2]

[1] PG Student, [2]Assistant Professor , Department of Computer Science and Engineering,

PRIST University, Trichy District, India

([1] m.venkat.trichy@gmail.com, [2] srajesh37@gmail.com)

Abstract

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be encrypted by the human visual system. The benefit of the visual secret sharing scheme is in its decryption process where without any complex cryptographic computation encrypted data is decrypted using Human Visual System (HVS). But the encryption technique needs cryptographic computation to divide the image into a number of parts let n. k-n secret sharing scheme is a special type of Visual Cryptographic technique where at least a group of k shares out of n shares reveals the secret information, less of it will reveal no information.

It uses the characteristics of human vision to decrypt the encrypted images. For security, it also ensures that hackers cannot perceive any clues about secret image from individual cover images. The encrypting technologies of traditional cryptography are usually used to protect information security. With such technologies, the data become disordered after being encrypted and can then be recovered by a correct key. Various methods available they are gray level and color images based on studies in black-and-white visual cryptography, the halftone technology, and the color decomposition method. WS-VSS schemes for color images that reproduce clearer images with a smaller pixel expansion compared to US-VSS scheme.

Index Terms — Visual Cryptography, Multi-Secrete Sharing.

I. INTRODUCTION

It is now common to transfer multimedia data via the Internet. With the coming era of electronic commerce, there is an urgent need to solve the problem of ensuring information safety in today's increasingly open network environment. The encrypting technologies of traditional cryptography are usually used to protect information security. With such Technologies, the data become disordered after being encrypted and can then be recovered by a correct key. Without the correct key, the encrypted source content can hardly be detected even unauthorized persons steal the information's.
WS-VSS schemes for color images that reproduce clearer images with a smaller pixel expansion compared to US-VSS scheme. Both VSS schemes for black–white binary secrete images a gap exists between two security notions. The text information is encrypted by ASCII values, or any special characters. It uses the characteristics of human vision to decrypt encrypted images.

The proposed technique ensures the security of visual information. The display employs a decoding mask based on Color Cryptography System. Without the decoding mask, the displayed information cannot be viewed. The viewing zone is limited by the decoding mask so that only one person can view the information. We have developed a set of encryption codes to maintain the designed viewing zone and have demonstrated a display that provides a limited viewing zone.

Ramp schemes in VSS schemes, in which a secret image is partially reproduced when the number of shares is below the threshold. Unfortunately, this may sometimes make it easy to guess whole secret images from a partial image since the secret is an *image* in VSS schemes.

The original clear text is revealed by placing the transparency with key over the page with the cipher text, even though each one of them is distinguishable from random noise. The system is similar to a one time pad in the sense that each page of cipher text is decrypted with a different transparency.

II. RELATED WORK

2.1 Project overview

The text information is encrypted by color palette images. Each user has created individual account, and then they access their required pages. The user's password is converting into ASCII format and stored into the database. So any hackers or admin also should not find out the particular user's password details. The user's information is protected into specific secret key entered by user. The secret key is converting into ASCII format and stored to database. Whenever the user has decrypted their encrypted information, they should enter the correct secret key. And user sends any secure information, it was encrypted and its link only sent to the mail.

- Basic theorem of visual cryptography

Because the output media of visual cryptography are transparencies, we treat the white pixels of black-and-white images as transparent. The black-and-white visual cryptography decomposes every pixel in a secret image into a 2×2 block in the two transparencies according to the rules. when a pixel is black, it chooses one of the other two combinations. The characteristics of two stacked pixels are: black and black is black, white and black is black, and white and white is white.

- The halftone technology

The way to represent the gray level of images is to use the density of printed dots. The method that uses the density of the net dots to simulate the gray level is called Halftone and transforms an image with gray level into a binary image before processing.

- Grey level visual cryptography

Most printers have to transform gray-level images into halftone ones before printing, and the transformed halftone images are black-and-white only, such an image format is very suitable for the traditional method to generate the shares of visual cryptography. Transformed halftone images to generate the visual cryptography for gray-level images. The algorithm is as follows:

1. Transform the gray-level image into a black-and-white halftone image.
2. For each black or white pixel in the halftone image, decompose it into a 2×2 block of the two transparencies according to the rules. If the pixel is white, randomly select one combination from the former two rows . If the pixel is black, randomly select one combination from the latter two rows as the content of the blocks in the two transparencies.
3. Repeat Step 2 until every pixel in the halftone image is decomposed, hence resulting in two transparencies of visual cryptography to share the secret image.

Scope of project

- The text information is encrypted by ASCII values for security.
- The original clear text is revealed by placing the transparency with key over the page with the cipher text.
- Visual Cryptography uses the characteristics of human vision to decrypt encrypted images.

2.2 Existing system

The existing system for this project the text information is encrypted by ASCII values, or any special characters. In the existing system, didn't use the safely sent the encrypted information into the mail. The hackers easily access that information. The encrypted text is didn't restrict any secret key. So that information easily decrypted.

- The existing system does not provide a friendly environment to encrypt or decrypt the data (images).
- The existing system supports with only one type of image format only.

2.2.1 Disadvantages

The proposed step construction generates VCSOR and VCSXOR which have optimal pixel expansion and contrast for each qualified set in the general access structure in most cases. Our scheme applies a technique to simplify the access structure, which can reduce the average pixel expansion (APE) in most cases compared with many of the results in the literature.

2.3 Proposed system

Proposed system Visual cryptography provides a friendly environment to deal with images. Generally cryptography tools supports only one kind of image formats. Our application supports .gif and .png formatted images and our application has been developed using swing and applet technologies, hence provides a friendly environment to users.

Whenever we transmit the data (image) in the network, any unauthenticated person can read our data (image). In order to provide security to data (image) generally sender will encrypt the data (image) and send it the intended person and the receiver will decrypt the encrypted data (image) and uses it.

In the proposed for this project, the text information is encrypted by color palette images. Each user has created individual account, and then they access their required pages. The user's password is converting into ASCII format and stored into the database. So any hackers or admin also should not find out the particular user's password details. The user's information is protected into specific secret key entered by user. The secret key is converting into

ASCII format and stored to database. Whenever the user has decrypted their encrypted information, they should enter the correct secret key. And user sends any secure information, it was encrypted and its link only sent to the mail.

2.3.1 Advantages

A method of encrypting and decrypting black-and-white images, including printed text, handwriting and photographs. Visual cryptography divides the pixels into two sets, which are printed on two acetate transparencies, known as the crypto sheet and key sheet. The crypto sheet and key sheet, alone, contain an apparently random pattern of pixels, but can be laid on top of one another to reveal the image.

2.4 LITERATURE REVIEW

2.4.1 A short survey on visual cryptography schemes

Visual Cryptography Schemes can decode concealed images based purely on human visual systems, without any aid from cryptographic computation. This nice property gives birth to a wide range of encryption applications. In this section, we will discuss how VCS is used in applications such as E-Voting system, financial documents and copyright protections.

Electronic-Balloting System: Nowadays, most of the voting are managed with computer systems. These voting machines expected voters to trust them, without giving proof that they recorded each vote correctly. One way to solve this problem is to issue receipts to voters to ensure them their votes are counted. However, this could improperly influence the voters, which produces coercion or vote selling problems. To solve this dilemma, Chaum [6] proposed a secret-Ballot Receipts system that is based on (2,2) threshold binary VCS. It generates an encrypted receipt to every voter which allows her to verify the election outcome - even if all election computers and records were compromised. At the polling station, you will receive a double-layer receipt that prints your voting decision. You will be asked to give one of the layer to the poll worker who will destroy it immediately with a paper shredder. The remaining one layer will now become unreadable. To make sure that your vote is not altered or deleted, you could querying the serial number on your receipt on the election Web site. This will return a posted receipt that looks identical to yours in hand. Notice that you do not need any software to verify this: simply print the posted receipt and overlaying it with your original receipt.

2.4.2 Visual cryptography schemes with optimal pixel Expansion

A visual cryptography scheme, each pixel of the secret image is subdivided into m subpixels. Hence, there is a loss of resolution proportional to m. Therefore, schemes with smaller pixel expansion are better. In the authors described a (2, n) threshold visual cryptography scheme having pixel expansion m such that

$m =(n-1)(n+3)\ \ 4$ if n is odd

$m=n(n+2)\ 4$ if n is even

It is immediate to see that the pixel expansion of the schemes presented in this paper is smaller.

2.4.3 Visual cryptography on Graphs

Algorithm for Finding Independent Star Forest Cover

The observation that given a k-coloring of G3, we can decompose G as follows:

Let Ki =S v has color i N(v). Note this is an independent star forest cover as an edge between N(v)and N(w) implies there is a path of at most length 3 between v and w which translates to an edge (v;w) in G3, hence they cannot be of the same color. Each edge is covered exactly twice.

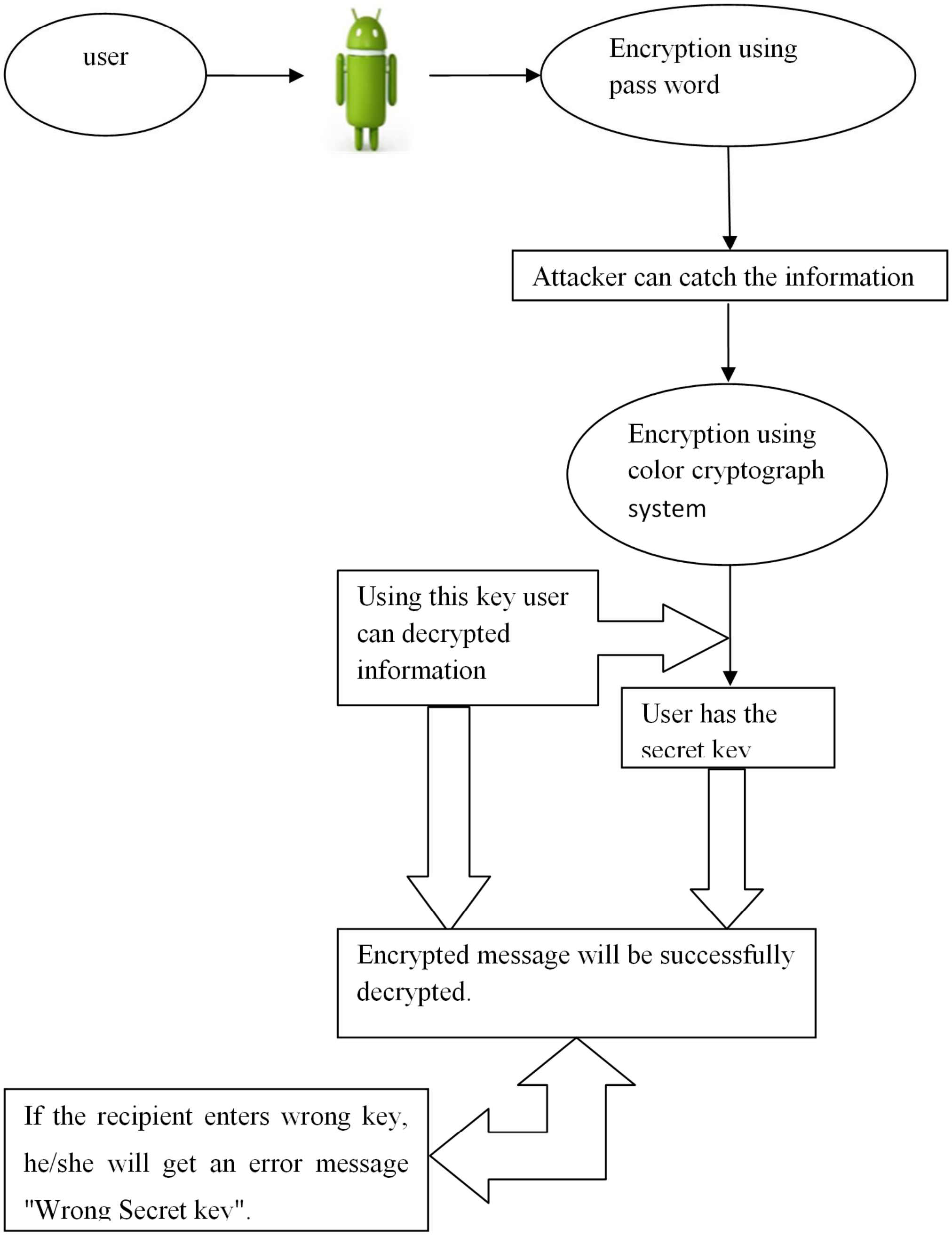
Our construction in the previous section can therefore theoretically be made with pixel expansion and contrast parameters dependent only on the chromatic number of G3 and the degree of G. It is NP-hard to the chromatic number, so instead we apply a less optimal solution to color the graph. We remodel the algorithm found in Luby [Lub86] into the algorithm in presented.

```
i →0
Construct G3 = (V;E)
while (V;E) is not empty do
i Ã i + 1
Find a Maximal Independent Set S
Color all the vertices in S by color i
V Ã V nS
end while
```

This algorithm will use at most *d*3 +1 colors (cf. [Lub86] Section 7) if *G* is of degree *d*. This is because at each stage if the node itself is not colored then at least one neighbor is colored (by the property of a maximal independent set). Thus at the next stage, its degree will drop by at least 1 and since each vertex in *G*3 has at most degree *d*3, we arrive at the conclusion of at most *d*3 + 1 colors.

Combining this algorithm with the construction from the previous section gives rise to a construction of a GEVCS on any graph, and for *d*-bounded degree graphs a constant-factor (on the order of *d*4) pixel expansion and contrast as stated in our main theorem. Unlike the naÄ³ve construction, this construction is independent of the number of participants.

2.5 DATA FLOW DIAGRAM



III. MODULES

- Create Color Palette Image
- Encrypt the Text
- Send the encrypted text to Mail with web links
- Retrieve the web links from mail
- Decrypt the Text

3.1 CREATE COLOR PALETTE IMAGE

In the module, small color images are created by PHP GD functions. Each text has assigned to particular images. The color palette images and its relevant information are stored into the database.

3.2 ENCRYPT THE TEXT

In this module the user has to register their name and their details. The registered information will be stored in the database. User or administrator tries to check this site and entered correct login username and password. After that, this application checks to redirects the required pages for administrator as well as user. The user has entered their important information, each text has convert to particular images. The images are randomly allocated to each text. Then image names only stored to database.

3.3 SEND THE ENCRYPTED TEXT TO MAIL WITH LINKS

In this module the user enter the information, and then send to particular mail address. User’s information is stored into the database for encrypted format. So web link with information’s ID only sent to the mail. The mail has sent by SMTP protocol. This process only worked on any online domain. Otherwise we will try to install the SMTP protocol.

3.4 RETRIEVE THE WEB LINKS FROM MAIL

In this module receiver is click this link, then open into this website. The receivers enter the secret key, if it is check with database, after they will retrieve the decrypted information.

3.5 DECRYPT THE TEXT

In this module the user’s secret information are stored into the database, these information displayed only color palette format. After the user is enter the secret key, if there are compare with database, and the information is decrypted. Then the user is view their information.

IV. CONCLUSION

Visual Cryptography provides one of the secure ways to transfer images on the Internet. The advantage of visual cryptography is that it exploits human eyes to decrypt secret images with no computation required. Unlike most studies of visual cryptography, which concentrate on black-and-white images, this paper exploits the techniques of halftone technology and color decomposition to construct three methods that can deal with both gray-level and color visual cryptography.

ACKNOWLEDGEMENT

I sincerely thanks to all authors in reference section. All papers in the reference section are very useful for my proposal. Their concepts, algorithms and techniques are very useful for my research.

REFERENCES

[1] M. Naor, A. Shamir, in: A. De Santis (Ed.), Visual Cryptography, Advances in Cryptology: Eurpocrypt'94, Lecture Notes in Computer Science, Vol. 950, Springer Berlin, 1995, pp. 1–12.

[2] M. Naor, A. Shamir, in: M. Lomas (Ed.), Visual Cryptography, II: Improving the Contrast via the Cover Base, Presented at Security in Communication Networks, AmalE,Italy, September 16–17, 1996. Lecture Notes in Computer Science, Vol. 1189, Springer, Berlin, 1997, pp. 197–202.Available also at Theory of Cryptography Library, Report 96-07, http://theory.lcs.mit.edu/□tcryptol/1996.html.

[3] D.R. Stinson, An introduction to visual cryptography, presented at Public Key Solutions '97, Toronto, Canada, April 28–30, 1997. http://bibd.unl.edu/□stinson/vcs-pus.ps

[4] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for general access structures, Inform. Comput
129 (1996) 86–106.

[5] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Extended schemes for visual cryptography, http://www.disi.unige.it/
person/AtenieseG

[6]O. Kafri and E. Keren. Encryption of pictures and shapes by random grids. Optics Letters, Vol. 12, Issue 6, pp. 377-379 (1987).

[7]B. Arazi, I. Dinstein, O. Kafri. Intuition, perception, and secure communication. IEEE Transactions on Systems, Man and Cybernetics. Vol. 19, Issue 5, pp. 1016-1020 (1989)

[8] Moni Naor and Adi Shamir, Visual Cryptography, EUROCRYPT 1994, pp1–12 IN Visual Cryptography on Cipher Machines & Cryptology

[9] Horng, G, Chen, T. and Tasi, D.S. Cheating in Visual Cryptography, Designs, Codes and Cryptography, 2006, pp219–236

[10] Cook, Richard C. (1960) Cryptographic process and enciphered product, United States patent 4,682,954.